5. Großübung

Aussagenlogik: Variablen repräsentieren Wahrheitswerte
Formeln " "

Prädikatenlogik: Variablen (& Terme) repräsentieren Daten
Formeln repräsentieren Wahrheitswerte
Prädikate transformieren
Daten zu Wahrheitswerten

Problem: Klare Trennung von

Syntax & Semantik notwendig.

Syntax: Aus welchen Symbolen besteht die Formel?

Semantik: Was bedeuten die Symbole?

Beispiel: Presburger Arithmetik

Syntax basiert auf der Signatur

Wir verwenden Infix- statt Präfixnotation, d.h. wir schreiben $(x+y)$ statt $+(x,y)$

$$S_{PA} = (\underbrace{\{\leq/_2\}}_{\text{Prädikatssymbol}}, \underbrace{\{0/_0, 1/_0, +/_2\}}_{\text{Funktionssymbole}})$$

$$A \equiv \exists x : \neg \exists y : x = y+1$$

Intuitiv: Es gibt eine Zahl, die keinen Vorgänger hat

Ist die Formel A wahr?

Können wir nicht sagen, da die Bedeutung der Symbole (noch) nicht festgelegt ist.

Betrachte die S_{PA}-Struktur

$M_{PA} = (\mathbb{N}, I_{PA})$ mit I „wie üblich" also

Symbol '0' natürliche Zahl 0

$$I_{PA}(0) = 0_{\mathbb{N}}$$
$$I_{PA}(1) = 1_{\mathbb{N}}$$
$$I_{PA}(+) = +_{\mathbb{N}}$$
$$I_{PA}(\leq) = \leq_{\mathbb{N}}$$

wie erwartet definiert

Nun können wir den Wahrheitswert

$$M_{PA}[\![A]\!]\sigma$$ ausrechnen.

beliebige Belegung der Variablen.
Welche genau spielt keine Rolle, da alle Variablen in A durch Quantoren gebunden sind.

$M_{PA}[\![A]\!]\sigma = 1$, denn

Notation auf den Folien: x/d

$M_{PA}[\![\neg\exists y: x=y+1]\!]\sigma\overbrace{\{x\mapsto 0\}}$

$= 1 - M_{PA}[\![\exists y: x=y+1]\!]\sigma\{x\mapsto 0\} = 1$, denn

$M_{PA}[\![\exists y: x=y+1]\!] = 0$, denn für alle $d\in\mathbb{N}$ gilt

$M_{PA}[\![\overbrace{x=y+1}^{\text{Formel}}]\!]\sigma\{x\mapsto 0, y\mapsto d\}$

$= \Big(\underbrace{M_{PA}[\![\overset{\text{Term}}{x}]\!]\sigma\{\ldots\}}_{\substack{=\sigma\{x\mapsto 0_{\mathbb{N}}, y\mapsto d\}(x)\\ = 0_{\mathbb{N}}}} = \underbrace{M_{PA}[\![\overbrace{y+1}^{\text{Term}}]\!]\sigma\{\ldots\}}_{\substack{= M_{PA}[\![y]\!]\sigma\{\ldots\} +_{\mathbb{N}} M_{PA}[\![1]\!]\sigma\{\ldots\}\\ =\sigma\{x\mapsto 0, y\mapsto d\}(y) +_{\mathbb{N}} 1_{\mathbb{N}}\\ = d +_{\mathbb{N}} 1_{\mathbb{N}}}}\Big)$

$= 0$, da $0 \neq d+1$ in $\mathbb{N}$, egal welchen Wert $d\in\mathbb{N}$ hat.

Um eine Aussage der Form

$M[\![\exists x: A]\!]\sigma = 1$ bzw. $M[\![\forall x: A]\!]\sigma = 0$

zu zeigen, reicht es, ein bestimmtes $d\in D_M$ aus dem Datenbereich zu wählen und dann zu zeigen, dass

$M[\![A]\!]\sigma\{x\mapsto d\} = 1$ bzw. $M[\![A]\!]\sigma\{x\mapsto d\} = 0$ gilt.

Um $M[\![\forall x: A]\!]\sigma = 1$ bzw. $M[\![\exists x: A]\!]\sigma = 0$

zu zeigen, muss dies für alle d, also für ein beliebiges d gezeigt werden.

$B \equiv \exists x \forall y : y \le x$

Intuitiv: Es gibt eine größte Zahl.

$M_{PA} [\![B]\!] \sigma = 0$, denn für $d \in \mathbb{N}$ beliebig gilt

$M_{PA} [\![\forall y : y \le x]\!]_{\sigma\{x \mapsto d\}} = 0$, denn für $y \mapsto \underbrace{d+1}_{\in \mathbb{N}}$ gilt

$M_{PA} [\![y \le x]\!] \sigma \{x \mapsto d, y \mapsto d+1\} \overset{\text{Zwischen-schritte}}{=} \ldots = ((d+1) \le_{\mathbb{N}} d) = 0$

Also $M_{PA} [\![A]\!] = 1$, $M_{PA} [\![B]\!] = 0$.

Es gibt jedoch andere S_{PA}-Strukturen, die zu anderen Wahrheitswerten führen:

$M_5 = (\{0,1,2,3,4\}, I_5)$

mit $I_5(0) = 0 \in \{0,\ldots,4\}$

$I_5(1) = 1 \in \{0,\ldots,4\}$

$I_5(\le) = \le_{\mathbb{N}}$ eingeschränkt auf $\{0,\ldots,4\}$

$I_5(+) = +_5$ mit $d +_5 e := (d +_{\mathbb{N}} e)$ modulo 5

Nun gilt

- $M_5 [\![A]\!] = 0$ // 0 hat 4 als Vorgänger: $0 = 4 +_5 1$
- $M_5 [\![B]\!] = 1$ // 4 ist größte Zahl.

Insb. A und B sind erfüllbar, aber keine Tautologien.

Der Presburger-Arithmetik fehlt im Vergleich zur „normalen" (Peano-) Arithmetik die Multiplikation.

Nachteil: Weniger Ausdrucksmächtig.

Vorteil: Algorithmik:

Es gibt ein Verfahren, dass zu einer gegebenen Formel A den Wahrheitswert

$$M_{PA}[\![A]\!]$$ ausrechnet *.

Dies gibt es nicht (und kann es nicht geben) für die normale Arithmetik

$$S_{Peano} = (\{\leq/2\}, \{0/0, 1/0, +/2, \cdot/2\})$$
$$M_{Peano} = (\mathbb{N}, I_{Peano}) \text{ mit } I_{Peano} \text{ „wie üblich".}$$

Formal: Das Bestimmen von

$$M_{Peano}[\![A]\!]$$

ist ein nicht-berechenbares Problem**.

---

*: Implementiert z.B. in Microsoft Z3

**: Siehe Vorlesung „Theoretische Informatik 2"

Formalisierung / Modellierung natursprachlicher Aussagen durch Prädikatenlogik

Bsp.: Barbier von Sevilla

1. Alle Männer in Sevilla sind rasiert
   (und zwar werden sie immer von der gleichen Person rasiert.)
2. Es gibt genau einen Barbier (in Sevilla, und dieser ist ein Mann.)
3. Der Barbier rasiert genau die Männer, die sich nicht selbst rasieren.

(Frage: Wer rasiert den Barbier?)

Modellierung:

Keine Funktionssymbole

$$S = (\{iB/_1, rV/_2\}, \emptyset)$$

Intuition:

- Datenwerte $\hat{=}$ Männer in Sevilla
- iB identifiziert Barbiere („ist Barbier")
- rV „rasiert von"

kurz für $\neg(z=y)$

$$A_1 \equiv \forall x (\exists y: rV(x,y) \wedge \forall z: z \neq y \rightarrow \neg rV(x,z))$$

$$A_2 \equiv \exists y: (iB(y) \wedge (\forall z: z \neq y \rightarrow \neg iB(z)))$$

$$A_3 \equiv \forall x: \underbrace{\neg rV(x,x)}_{\text{rasiert sich nicht selbst}} \leftrightarrow \underbrace{(\exists y: rV(x,y) \wedge iB(y))}_{\text{wird vom Barbier rasiert}}$$

Es gibt verschiedene Modellierungsmöglichkeiten

- mit iB als 0-stelligem Funktionssymbol
- ganz ohne iB.

$\{A_1, A_2, A_3\}$ ist eine <u>unerfüllbare</u> Formelmenge.
Egal wie M, also Daten & Interpretationen, gewählt werden, es gilt immer $M[\![A_1 \wedge A_2 \wedge A_3]\!] = 0$.

Tatsächlich ist bereits die folgende abgeschwächte Version von A_3 <u>unerfüllbar</u>:

$$A \equiv \exists y\, \forall x : \neg rV(x,x) \leftrightarrow rV(x,y)$$

„Es gibt einen, der genau die rasiert, die sich nicht selbst rasieren."

Beweis:

Angenommen es gäbe S-Struktur M mit

$$M[\![A]\!]\sigma = 1.$$

Dann gibt es einen Datenwert B mit // „∃"-Quantor

$$M[\![\forall x : \neg rV(x,x) \leftrightarrow rV(x,y)]\!]\sigma\{y \mapsto B\} = 1$$

Wir wählen nun auch für x den Wert B, // erlaubt, da „∀"-Quantor
und erhalten

$$M[\![\neg rV(x,x) \leftrightarrow rV(x,y)]\!]\sigma\{y \mapsto B, x \mapsto B\} = 1$$

$$\parallel$$

$$\text{"}\neg rV^M(B,B) \leftrightarrow rV^M(B,B)\text{"}$$

$\parallel$ – egal ob $rV^M(B,B)=0$ oder ... $= 1$

$$0$$

Widerspruch

Also: $M[\![A]\!]\sigma = 0$ für alle M.

Da $\{A_1, A_2, A_3\} \models A$, ist auch $\{A_1, -, A_3\}$ unerfüllbar.

(Ang. $M[\![A_1 \wedge A_2 \wedge A_3]\!]\sigma = 1$, dann wegen $\{A_1, A_2, A_3\} \models A$ auch $M[\![A]\!]\sigma = 1$, Widerspruch.)

Der „Barbier von Sevilla" ist die natursprachliche Version der Ru~~ss~~sel-Antinomie (1903), einem Paradoxon, das zeigt, dass ein naiver Begriff von Menge („Zusammenfassung von [..] Objekten unserer Vorstellung") nicht zu einem konsistenten Aufbau der Mathematik führt.

Moderne Axiomatisierungen vermeiden das Parodoxon ($\leadsto$ „Aussonderungsaxiom")

Prädikatenlogischer Aufbau der Mathematik

Was ist Mathematik? Wann ist eine Aussage wahr?
Was ist ein Beweis?

Seit ~1900: Verwendung von Prädikatenlogik
„Axiomatisierung"

Vorgehensweise:
- Wähle Signatur ~~en~~ S // lege Syntax fest
- Wähle Axiome, Formelmenge Γ // Als wahr angenommene Formel (ohne Beweis)

Nun:
Formel A wahr $:\Leftrightarrow$ $\Gamma \models A$ gilt
Formel A falsch $:\Leftrightarrow$ $\Gamma \models \neg A$ gilt.*
Beweis, dass A wahr $:\Leftrightarrow$ Beweis von $\Gamma \models A$ in einem geeigneten Kalkül (ähnlich wie K_0)

---

*: Was ist, wenn weder $\Gamma \models A$, noch $\Gamma \models \neg A$?
Kann das vorkommen? JA!
Beispielsweise kann die Kontinuumshypothese
$$\exists \text{ Menge } X: |\mathbb{N}| < |X| < |\mathbb{R}|$$
in der gängigen ZFC-Axiomatisierung weder bewiesen, noch widerlegt werden.

Diese Vorgehensweise erklärt auch den Namen Mathematik – Kunst des Lernens (altgriechisch)

„Welche Aussagen werden zwangsläufig klar, wenn wir gewisse Axiome als wahr annehmen?"

Heute: Mengentheoretischer Aufbau der Mathematik

Alle Mathematischen Objekte sind Mengen (auch Zahlen, Funktionen, ...)

Wenige verschiedene Axiomatisierungen, am weitesten verbreitet ist ZF(C),

Z – Zermelo, F – Fraenkel, C – Auswahlaxiom (C ≙ Choice)

Die komplette ~~Ma~~ Mathematik kann aus 10 Axiomen (schemata) abgeleitet werden.

Hinweis: Wir haben nirgends eine „Semantik der Mathematik" definiert. In der Tat, $\Gamma \models A$ bedeutet, dass jede Struktur (Semantik), die Γ erfüllt, auch A erfüllt.

Vorteil: Wir müssen nicht definieren, was eine Menge ist.

Nachteil: Es ist nicht klar, ob z.B. ZFC konsistent (erfüllbar) ist.

__Bsp__:

Verwende Signatur $S = (\{\in/2\}, \emptyset)$ „ist Element von" / einziges Prädikat; keine Funktionen

Axiome:

- $\exists x \forall y: \neg(y \in x)$

  Existenz der leeren Menge $\emptyset$

- $\forall x \forall y \exists \underset{\{x,y\}}{z}: \forall w: (w \in z \leftrightarrow (w = x \vee w = y))$

  Zu zwei Mengen x, y gibt es auch die Menge $\{x, y\}$

  Erlaubt die Konstruktion von

  $\{\emptyset, \emptyset\} = \{\emptyset\}$

  $\{\{\emptyset\}, \emptyset\}$

  $\{\{\emptyset\}, \{\emptyset\}\} = \{\{\emptyset\}\}$ usw.

  Erlaubt die Definition der natürlichen Zahlen

  $0 := \emptyset$

  $n+1 := n \cup \{n\} = \{0, \dots, n\}$

  z.B.

  $0 = \emptyset$, $1 = \{\overset{0}{\emptyset}\}$, $2 = \{\overset{1}{\{\emptyset\}}, \overset{0}{\emptyset}\}$

  $3 = \{\overset{2}{\{\{\emptyset\}, \emptyset\}}, \overset{1}{\{\emptyset\}}, \overset{0}{\emptyset}\}$, usw.

- $\forall x \forall y \exists \underset{x \cup y}{z}: \forall w: (w \in z \leftrightarrow (w \in x \vee w \in y))$*

  Zu zwei Mengen x, y gibt es auch die Vereinigung $x \cup y = \{w \mid w \in x \text{ oder } w \in y\}$

---

*: Tatsächlich verwendet ZF(C) die Verallgemeinerte Version

$$\forall x \exists z: \forall w: (w \in z \leftrightarrow (\exists y: w \in y \wedge y \in x))$$

+ 4 weitere Axiome (Gleichheit, Potenzmenge, Fundierung, Existenz von $\mathbb{N}$)
+ 2 Axiomenschemata (Aussonderung, Ersetzung)
+ Auswahlaxiom.